Docket No. 242895US2SRD

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

IN RE APPLICATION OF: Hideo SHIMIZU, et al. GAU:

SERIAL NO: NEW APPLICATION EXAMINER:

FILED: HEREWITH

FOR: POLYNOMIAL INVERSE COMPUTING APPARATUS, MULTIPLIER APPARATUS AND POLYNOMIAL INVERSE COMPUTING METHOD

REQUEST FOR PRIORITY

COMMISSIONER FOR PATENTS
ALEXANDRIA, VIRGINIA 22313

SIR:

☐ Full benefit of the filing date of U.S. Application Serial Number , filed , is claimed pursuant to the provisions of **35 U.S.C. §120**.

☐ Full benefit of the filing date(s) of U.S. Provisional Application(s) is claimed pursuant to the provisions of **35 U.S.C. §119(e)**: **Application No.** **Date Filed**

■ Applicants claim any right to priority from any earlier filed applications to which they may be entitled pursuant to the provisions of **35 U.S.C. §119**, as noted below.

In the matter of the above-identified application for patent, notice is hereby given that the applicants claim as priority:

COUNTRY	APPLICATION NUMBER	MONTH/DAY/YEAR
Japan	2002-287860	September 30, 2002

Certified copies of the corresponding Convention Application(s)

■ are submitted herewith

☐ will be submitted prior to payment of the Final Fee

☐ were filed in prior application Serial No. filed

☐ were submitted to the International Bureau in PCT Application Number
Receipt of the certified copies by the International Bureau in a timely manner under PCT Rule 17.1(a) has been acknowledged as evidenced by the attached PCT/IB/304.

☐ (A) Application Serial No.(s) were filed in prior application Serial No. filed ; and

☐ (B) Application Serial No.(s)

- ☐ are submitted herewith
- ☐ will be submitted prior to payment of the Final Fee

Respectfully Submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.

Marvin J. Spivak
Registration No. 24,913
C. Irvin McClelland
Registration Number 21,124

Customer Number
22850
Tel. (703) 413-3000
Fax. (703) 413-2220
(OSMMN 05/03)

03S0186

日　本　国　特　許　庁
JAPAN　PATENT　OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application:　２００２年　９月３０日

出願番号
Application Number:　特願２００２－２８７８６０

[ST.10/C]:　[ＪＰ２００２－２８７８６０]

出願人
Applicant(s):　株式会社東芝

２００３年　２月２１日

特許庁長官
Commissioner,
Japan Patent Office　太田信一郎

出証番号　出証特２００３－３００９７０７

【書類名】　特許願
【整理番号】　A000202891
【提出日】　平成14年 9月30日
【あて先】　特許庁長官　殿
【国際特許分類】　G06F 15/00
【発明の名称】　逆元計算装置及び逆元計算方法
【請求項の数】　11
【発明者】
【住所又は居所】　神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内
【氏名】　清水　秀夫
【発明者】
【住所又は居所】　神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内
【氏名】　新保　淳
【特許出願人】
【識別番号】　000003078
【氏名又は名称】　株式会社　東芝
【代理人】
【識別番号】　100058479
【弁理士】
【氏名又は名称】　鈴江　武彦
【電話番号】　03-3502-3181
【選任した代理人】
【識別番号】　100084618
【弁理士】
【氏名又は名称】　村松　貞男
【選任した代理人】
【識別番号】　100068814

【弁理士】

【氏名又は名称】　坪井　淳

【選任した代理人】

【識別番号】　100092196

【弁理士】

【氏名又は名称】　橋本　良郎

【選任した代理人】

【識別番号】　100091351

【弁理士】

【氏名又は名称】　河野　哲

【選任した代理人】

【識別番号】　100088683

【弁理士】

【氏名又は名称】　中村　誠

【選任した代理人】

【識別番号】　100070437

【弁理士】

【氏名又は名称】　河井　将次

【手数料の表示】

【予納台帳番号】　011567

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　逆元計算装置及び逆元計算方法

【特許請求の範囲】

【請求項１】

第１乃至第６のレジスタと、左シフト回路と、排他的論理和回路と、標数２の拡大体での２倍演算を施す２倍演算回路と、標数２の拡大体での１／２倍演算を施す１／２倍演算回路と、レジスタの内容が０か否か判定する判定回路と、レジスタの内容をデクリメントするデクリメント回路と、レジスタの内容をインクリメントするインクリメント回路と、それらを制御する制御回路とを用いて構成したことを特徴とする逆元計算装置。

【請求項２】

初期値として除数を格納する第１のレジスタと、

初期値として法を格納し、所定の場合に前記第１のレジスタの内容を保持する第２のレジスタと、

初期値として被除数を格納する第３のレジスタと、

初期値として０を格納し、所定の場合に前記第３のレジスタの内容を保持し、最終的に計算結果を保持する第４のレジスタと、

初期値として法のビット数を格納する第５のレジスタと、

初期値として０を格納する第６のレジスタと、

所定の場合に前記第１のレジスタを左シフトする左シフト回路と、

所定の場合に前記第１のレジスタと前記第２のレジスタの排他的論理和を求めて該第１のレジスタへ出力する第１の排他的論理和回路と、

所定の場合に前記第３のレジスタに対して標数２の拡大体での２倍演算を施す２倍演算回路と、

所定の場合に前記第４のレジスタに対して標数２の拡大体での１／２倍演算を施す１／２倍演算回路と、

所定の場合に前記第３のレジスタと前記第４のレジスタの排他的論理和を求め該第３のレジスタへ出力する第２の排他的論理和回路と、

所定の場合に前記第５のレジスタが０か否か判定する第１の判定回路と、

所定の場合に前記第５のレジスタをデクリメントする第１のデクリメント回路と、

所定の場合に前記第６のレジスタが０か否かを判定する第２の判定回路と、

所定の場合に前記第６のレジスタをデクリメントする第２のデクリメント回路と、

所定の場合に前記第６のレジスタをインクリメントするインクリメント回路とを備えたことを特徴とする逆元計算装置。

【請求項３】

第１の状態においては、前記第１のレジスタの最上位ビットが１でない限りは、前記第１のレジスタを前記左シフト回路により左シフトし、前記第３のレジスタを前記２倍演算回路により２倍し、前記第５のレジスタを前記第１のデクリメント回路により１だけデクリメントし、前記第６のレジスタを前記インクリメント回路により１だけインクリメントする一連の処理を繰り返し行い、前記第１のレジスタの最上位ビットが１であるときは、第２の状態に状態遷移し、

第２の状態においては、前記第１のレジスタ及び前記第２のレジスタにそれぞれ前記第１の排他的論理和回路の出力及び該第１のレジスタの内容を格納するとともに、前記第３のレジスタ及び前記第４のレジスタにそれぞれ前記第２の排他的論理和回路の出力及び該第３のレジスタの内容を格納し、その後に第３の状態に状態遷移し、

第３の状態においては、前記第２の判定回路により前記第６のレジスタが０でないと判定される限り、まず、前記第１のレジスタの最上位ビットが１である場合にのみ、該第１のレジスタに前記第１の排他的論理和回路の出力を格納するとともに、前記第３のレジスタに前記第２の排他的論理和回路の出力を格納し、次いで、前記第６のレジスタを前記第２のデクリメント回路により１だけデクリメントし、前記第１のレジスタを前記左シフト回路により左シフトし、前記第４のレジスタを前記１／２倍演算回路により１／２倍する一連の処理を繰り返し行い、前記第２の判定回路により前記第６のレジスタが０になったと判定されたときは、前記第１の判定回路により前記第５のレジスタが０でないと判定されたならば、前記第１の状態に状態遷移し、０であると判定されたならば、前記第４レジ

スタの内容を結果として出力することを特徴とする請求項２に記載の逆元計算装置。

【請求項４】

前記２倍演算回路は、前記第３のレジスタの最上位ビットが１である場合には、前記第３のレジスタを１ビットだけ左シフトした後に、前記法との排他的論理和を取り、前記第３のレジスタの最上位ビットが０である場合には、前記第３のレジスタを１ビットだけ左シフトするものであることを特徴とする請求項１ないし３のいずれか１項に記載の逆元計算装置。

【請求項５】

前記１／２倍演算回路は、前記第４のレジスタの最下位ビットが１である場合には、前記法との排他的論理和を取った後に、１ビットだけ右シフトし、前記第４のレジスタの最下位ビットが０である場合には、前記第４のレジスタを１ビットだけ右シフトするものであることを特徴とする請求項１ないし４のいずれか１項に記載の逆元計算装置。

【請求項６】

前記第５のレジスタをワンホットカウンタで実現したことを特徴とする請求項１ないし５のいずれか１項に記載の逆元計算装置。

【請求項７】

前記第６のレジスタをワンホットカウンタで実現したことを特徴とする請求項１ないし６のいずれか１項に記載の逆元計算装置。

【請求項８】

請求項１ないし７のいずれか１項に記載の前記第１及び第３乃至第５のレジスタ、前記左シフト回路、前記第１又は第２の排他的論理和回路、前記２倍演算回路、前記第１又は第２の判定回路並びに前記第１又は第２のデクリメント回路を、前記逆元計算装置と共用し、

前記第１及び第３乃至第５のレジスタに初期値としてそれぞれ乗数、０、被乗数、法のビット数を格納し、

前記第１又は第２の判定回路により前記第５のレジスタが０でないと判定される限り、前記第５のレジスタを前記第１又は第２のデクリメント回路により１だ

けデクリメントし、前記第３のレジスタを前記２倍演算回路により２倍し、前記第１のレジスタを前記左シフト回路により左シフトし、前記第１のレジスタの最上位ビットが１である場合にのみ、前記第３のレジスタに、該第３のレジスタと前記第４のレジスタを入力とする前記第１又は第２の排他的論理和回路の出力を格納する一連の処理を繰り返し行い、前記第１又は第２の判定回路により前記第５のレジスタが０になったと判定されたときは、前記第３レジスタの内容を結果として出力することを特徴とする乗算装置。

【請求項９】

第１乃至第６のレジスタに初期値としてそれぞれ除数、法、被除数、０、法のビット数及び０を格納し、

第１の状態においては、前記第１のレジスタの最上位ビットが１でない限りは、前記第１のレジスタを左シフト回路により左シフトし、前記第３のレジスタに対して２倍演算回路により標数２の拡大体での２倍演算を施し、前記第５のレジスタを第１のデクリメント回路により１だけデクリメントし、前記第６のレジスタをインクリメント回路により１だけインクリメントする一連の処理を繰り返し行い、前記第１のレジスタの最上位ビットが１であるときは、第２の状態に状態遷移し、

第２の状態においては、前記第１のレジスタ及び前記第２のレジスタにそれぞれ該第１のレジスタと該第２のレジスタを入力とする第１の排他的論理和回路の出力及び該第１のレジスタの内容を格納するとともに、前記第３のレジスタ及び前記第４のレジスタにそれぞれ該第３のレジスタと該第４のレジスタを入力とする第２の排他的論理和回路の出力及び該第３のレジスタの内容を格納し、その後に第３の状態に状態遷移し、

第３の状態においては、前記第６のレジスタが０でない限り、まず、前記第１のレジスタの最上位ビットが１である場合にのみ、該第１のレジスタに前記第１の排他的論理和回路の出力を格納するとともに、前記第３のレジスタに前記第２の排他的論理和回路の出力を格納し、次いで、前記第６のレジスタを第２のデクリメント回路により１だけデクリメントし、前記第１のレジスタを前記左シフト回路により左シフトし、前記第４のレジスタに対して１／２倍演算回路により標

数２の拡大体での１／２倍演算を施す一連の処理を繰り返し行い、前記第６のレジスタが０になったときは、前記第５のレジスタが０でないならば、前記第１の状態に状態遷移し、０であるならば、前記第４レジスタの内容を結果として出力することを特徴とする逆元計算方法。

【請求項１０】

前記２倍演算では、前記第３のレジスタの最上位ビットが１である場合には、前記第３のレジスタを１ビットだけ左シフトした後に、前記法との排他的論理和を取り、前記第３のレジスタの最上位ビットが０である場合には、前記第３のレジスタを１ビットだけ左シフトすることを特徴とする請求項９に記載の逆元計算方法。

【請求項１１】

前記１／２倍演算では、前記第４のレジスタの最下位ビットが１である場合には、前記法との排他的論理和を取った後に、１ビットだけ右シフトし、前記第４のレジスタの最下位ビットが０である場合には、前記第４のレジスタを１ビットだけ右シフトすることを特徴とする請求項９または１０に記載の逆元計算方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、ＶＬＳＩ実装に適した標数２のガロア体での逆元計算装置及び逆元計算方法に関する。

【０００２】

【従来の技術】

標数２のガロア体は符号理論や楕円曲線暗号等の様々な工業分野に応用されてる。標数２のガロア体の元の逆元の計算は標数２の楕円曲線上の有理点の加算に必要とされる演算である。

【０００３】

任意の体の元の逆元を計算するアルゴリズムとしては、拡張ユークリッドアルゴリズムが知られている。しかし、拡張ユークリッドアルゴリズムは乗算と除算を必要とするため、ハードウェアで実装した際には実行ステップ数や回路規模が

大きくなるという問題があった。

【０００４】

１９８７年にＳｔｅｉｎは乗算と除算がいらない拡張ユークリッドアルゴリズムの改良を提案している。この改良により、標数２のガロア体の逆元は、シフト演算、排他的論理和、２つの多項式の最高次数の比較回路、多項式が定数であるかの判定回路及び制御回路により構成できる。

【０００５】

一般にＶＬＳＩの性能は、実行サイクル数（レイテンシ）、回路規模、回路遅延の３つにより決まる。法多項式の最高次数をｍとすると、Ｓｔｅｉｎのアルゴリズムではレイテンシは２ｍステップであり、理論的にこれ以上の高速化は望めない。回路規模はＯ（ｍ）であり、回路遅延はＯ（ｌｏｇ　ｍ）である。上で列挙したうち、２つの多項式の最高次数の比較回路と多項式が定数であるかの判定回路の２つが回路規模と回路遅延の両方を大きくしている。楕円曲線暗号への応用では、ｍは数百程度である。

【０００６】

その他、種々のガロア体逆元演算の高速化が提案されている（例えば、下記特許文献１～４参照）。

【０００７】

【特許文献１】

特開２０００－０４７８３３号公報

【０００８】

【特許文献２】

特開２０００－３１５２０１号公報

【０００９】

【特許文献３】

特開２０００－３２２２８０号公報

【００１０】

【特許文献４】

特開２００２－０２３９９９号公報

【００１１】

【発明が解決しようとする課題】

従来知られていた標数２のガロア体での逆元計算アルゴリズムであるＳｔｅｉｎのアルゴリズムでは、ＶＬＳＩ化した際に回路規模と回路遅延が大きくなる問題があった。

【００１２】

本発明は、上記事情を考慮してなされたもので、標数２のガロア体での逆元計算アルゴリズムをＶＬＳＩ化した際、回路規模や回路遅延を従来よりも小さく抑えることができる逆元計算装置及び逆元計算方法を提供することを目的とする。

【００１３】

また、本発明は、標数２のガロア体での逆元計算アルゴリズムをＶＬＳＩ化した際、逆元計算装置と大部分の部品を共通に利用することができる乗算装置を提供することを目的とする。

【００１４】

【課題を解決するための手段】

本発明に係る逆元計算装置は、第１乃至第６のレジスタと、左シフト回路と、排他的論理和回路と、標数２の拡大体での２倍演算を施す２倍演算回路と、標数２の拡大体での１／２倍演算を施す１／２倍演算回路と、レジスタの内容が０か否か判定する判定回路と、レジスタの内容をデクリメントするデクリメント回路と、レジスタの内容をインクリメントするインクリメント回路と、それらを制御する制御回路とを用いて構成したことを特徴とする。

【００１５】

また、本発明に係る逆元計算装置は、初期値として除数を格納する第１のレジスタと、初期値として法を格納し、所定の場合に前記第１のレジスタの内容を保持する第２のレジスタと、初期値として被除数を格納する第３のレジスタと、初期値として０を格納し、所定の場合に前記第３のレジスタの内容を保持し、最終的に計算結果を保持する第４のレジスタと、初期値として法のビット数を格納する第５のレジスタと、初期値として０を格納する第６のレジスタと、所定の場合に前記第１のレジスタを左シフトする左シフト回路と、所定の場合に前記第１の

レジスタと前記第２のレジスタの排他的論理和を求めて該第１のレジスタへ出力する第１の排他的論理和回路と、所定の場合に前記第３のレジスタに対して標数２の拡大体での２倍演算を施す２倍演算回路と、所定の場合に前記第４のレジスタに対して標数２の拡大体での１／２倍演算を施す１／２倍演算回路と、所定の場合に前記第３のレジスタと前記第４のレジスタの排他的論理和を求め該第３のレジスタへ出力する第２の排他的論理和回路と、所定の場合に前記第５のレジスタが０か否か判定する第１の判定回路と、所定の場合に前記第５のレジスタをデクリメントする第１のデクリメント回路と、所定の場合に前記第６のレジスタが０か否かを判定する第２の判定回路と、所定の場合に前記第６のレジスタをデクリメントする第２のデクリメント回路と、所定の場合に前記第６のレジスタをインクリメントするインクリメント回路とを備えたことを特徴とする。

【００１６】

好ましくは、第１の状態においては、前記第１のレジスタの最上位ビットが１でない限りは、前記第１のレジスタを前記左シフト回路により左シフトし、前記第３のレジスタを前記２倍演算回路により２倍し、前記第５のレジスタを前記第１のデクリメント回路により１だけデクリメントし、前記第６のレジスタを前記インクリメント回路により１だけインクリメントする一連の処理を繰り返し行い、前記第１のレジスタの最上位ビットが１であるときは、第２の状態に状態遷移し、第２の状態においては、前記第１のレジスタ及び前記第２のレジスタにそれぞれ前記第１の排他的論理和回路の出力及び該第１のレジスタの内容を格納するとともに、前記第３のレジスタ及び前記第４のレジスタにそれぞれ前記第２の排他的論理和回路の出力及び該第３のレジスタの内容を格納し、その後に第３の状態に状態遷移し、第３の状態においては、前記第２の判定回路により前記第６のレジスタが０でないと判定される限り、まず、前記第１のレジスタの最上位ビットが１である場合にのみ、該第１のレジスタに前記第１の排他的論理和回路の出力を格納するとともに、前記第３のレジスタに前記第２の排他的論理和回路の出力を格納し、次いで、前記第６のレジスタを前記第２のデクリメント回路により１だけデクリメントし、前記第１のレジスタを前記左シフト回路により左シフトし、前記第４のレジスタを前記１／２倍演算回路により１／２倍する一連の処理

を繰り返し行い、前記第２の判定回路により前記第６のレジスタが０になったと判定されたときは、前記第１の判定回路により前記第５のレジスタが０でないと判定されたならば、前記第１の状態に状態遷移し、０であると判定されたならば、前記第４レジスタの内容を結果として出力するようにしてもよい。

【００１７】

また、本発明に係る乗算装置は、請求項１ないし７のいずれか１項に記載の前記第１及び第３乃至第５のレジスタ、前記左シフト回路、前記第１又は第２の排他的論理和回路、前記２倍演算回路、前記第１又は第２の判定回路並びに前記第１又は第２のデクリメント回路を、前記逆元計算装置と共用し、前記第１及び第３乃至第５のレジスタに初期値としてそれぞれ乗数、０、被乗数、法のビット数を格納し、前記第１又は第２の判定回路により前記第５のレジスタが０でないと判定される限り、前記第５のレジスタを前記第１又は第２のデクリメント回路により１だけデクリメントし、前記第３のレジスタを前記２倍演算回路により２倍し、前記第１のレジスタを前記左シフト回路により左シフトし、前記第１のレジスタの最上位ビットが１である場合にのみ、前記第３のレジスタに、該第３のレジスタと前記第４のレジスタを入力とする前記第１又は第２の排他的論理和回路の出力を格納する一連の処理を繰り返し行い、前記第１又は第２の判定回路により前記第５のレジスタが０になったと判定されたときは、前記第３レジスタの内容を結果として出力することを特徴とする。

【００１８】

また、本発明に係る逆元計算方法は、第１乃至第６のレジスタに初期値としてそれぞれ除数、法、被除数、０、法のビット数及び０を格納し、第１の状態においては、前記第１のレジスタの最上位ビットが１でない限りは、前記第１のレジスタを左シフト回路により左シフトし、前記第３のレジスタに対して２倍演算回路により標数２の拡大体での２倍演算を施し、前記第５のレジスタを第１のデクリメント回路により１だけデクリメントし、前記第６のレジスタをインクリメント回路により１だけインクリメントする一連の処理を繰り返し行い、前記第１のレジスタの最上位ビットが１であるときは、第２の状態に状態遷移し、第２の状態においては、前記第１のレジスタ及び前記第２のレジスタにそれぞれ該第１の

レジスタと該第２のレジスタを入力とする第１の排他的論理和回路の出力及び該第１のレジスタの内容を格納するとともに、前記第３のレジスタ及び前記第４のレジスタにそれぞれ該第３のレジスタと該第４のレジスタを入力とする第２の排他的論理和回路の出力及び該第３のレジスタの内容を格納し、その後に第３の状態に状態遷移し、第３の状態においては、前記第６のレジスタが０でない限り、まず、前記第１のレジスタの最上位ビットが１である場合にのみ、該第１のレジスタに前記第１の排他的論理和回路の出力を格納するとともに、前記第３のレジスタに前記第２の排他的論理和回路の出力を格納し、次いで、前記第６のレジスタを第２のデクリメント回路により１だけデクリメントし、前記第１のレジスタを前記左シフト回路により左シフトし、前記第４のレジスタに対して１／２倍演算回路により標数２の拡大体での１／２倍演算を施す一連の処理を繰り返し行い、前記第６のレジスタが０になったときは、前記第５のレジスタが０でないならば、前記第１の状態に状態遷移し、０であるならば、前記第４レジスタの内容を結果として出力することを特徴とする。

【００１９】

なお、装置に係る本発明は方法に係る発明としても成立し、方法に係る本発明は装置に係る発明としても成立する。

また、装置または方法に係る本発明は、コンピュータに当該発明に相当する手順を実行させるための（あるいはコンピュータを当該発明に相当する手段として機能させるための、あるいはコンピュータに当該発明に相当する機能を実現させるための）プログラムとしても成立し、該プログラムを記録したコンピュータ読取り可能な記録媒体としても成立する。

【００２０】

本発明によれば、標数２のガロア体での逆元計算アルゴリズムをＶＬＳＩ化した際、回路規模や回路遅延を従来よりも小さく抑えることができるようになる。例えば、法となる多項式の最高次数をｍとしたとき、従来方法のｃｉｒｃｕｉｔ ｄｅｐｔｈは、ｌｏｇ ｍであったが、本発明によれば、ｌｏｇ ｌｏｇ ｍに削減することができる。

【００２１】

また、本発明によれば、全てのシフト操作が、１ビット固定シフトとなる、という利点が得られる。

【００２２】

また、本発明によれば、逆元計算装置と乗算装置とで大部分の部品を共通に利用することができる。

【００２３】

【発明の実施の形態】

以下、図面を参照しながら発明の実施の形態を説明する。

【００２４】

法をＧとして、ＧＦ（２）の拡大体でのＡの逆元の計算を行うためのアルゴリズムを以下に示す。

【００２５】

法Ｇ（Ｇはｍ次多項式），ｍ，除数ａ（ａは次数がｍより小さい多項式），非除数ｂ（ｂは次数がｍより小さい多項式）は、入力として与える。

【００２６】

初期値として、下記のようにする。

Ａ＝ａ（Ａはｍ次多項式）

Ｂ＝ｂ（Ｂはｍ次多項式）

Ｃ＝Ｇ（Ｃはｍ次多項式）

Ｄ＝０（Ｄはｍ次多項式）

ｎ＝０（ｎはｍ以下の整数を表せる変数）

なお、本アルゴリズムは、アルゴリズムが完了したときのＤが、演算結果A^{-1}・Ｂを与えるものである。従って、Ａの逆元の計算の場合には、Ｂの初期値すなわちｂを１とする。本アルゴリズムによって、逆元計算だけしか行わない場合には、ｂを入力とせずに、Ｂの初期値を１に固定してもよい。

【００２７】

本アルゴリズムの記述は以下のとおりである。なお、下記のアルゴリズムにおいて、ｍｓｂ（Ａ）は、Ａの最高次の係数を意味する。また、ｌｅｆｔ＿ｓｈｉｆｔ（Ａ）は、多項式ＡにＸを掛けてＸ＾ｍで割った剰余を意味する。また、ｔ

ｗｉｃｅ（Ｂ）は、多項式ＢにＸを掛けて法多項式Ｇで割った剰余を意味する。また、ｈａｌｆ（Ｄ）は、多項式Ｄに１／Ｘを掛けて法多項式Ｇで割った剰余を意味する。

【００２８】

＜逆元計算アルゴリズム１＞

```
G, m, a, bの入力
A, B, C, D, nの初期化
while m ≠ 0
  // step 1
  while msb(A) = 0
    m ← m-1;
    n ← n+1;
    A ← left_shift(A);
    B ← twice(B);
  wend
  // step 2
  (A, C) ← (A xor C, A);
  (B, D) ← (B xor D, B);
  // step 3
  while n ≠ 0
    if msb(A) = 1 then (A, B) ← (A xor C, B xor D)
    n ← n-1
    A ← left_shift(A)
    D ← half(D)
  wend
wend
Dを出力
```

＜逆元計算アルゴリズム１＞

以上のアルゴリズムの記述をフローチャートの形で表したのが図１である。

【００２９】

ここで、ｍ－１次多項式を、図２のように係数を並べて表現することにする。例えば、法をx^4+x+1とすると、x^4+x+1は（1,0,0,1,1）で表され、$x+1$は(0,0,0,1,1)で表され、x^3+x^2+1は（0,1,1,1,0）で表され、０は（0,0,0,0,0）で表され、１は（0,0,0,0,1）で表される。

【００３０】

この場合、ｌｅｆｔ＿ｓｈｉｆｔ（Ａ）は、図３のように表現できる。

また、ｔｗｉｃｅ（Ａ）は、図４のように表現できる。なお、ステップＳ１２，Ｓ１３のA<<1は、Ａを左に１ビットだけシフトすることを表す。

また、ｈａｌｆ（Ａ）は、図５のように表現できる。なお、ステップＳ１５，Ｓ１６のA>>1は、Ａを右に１ビットだけシフトすることを表す。

【００３１】

図６に、法$G=x^4+x+1$とし、$a=x+1$としたときのａの逆元を求める場合、すなわち$(x+1)^{-1} \mod (x^4+x+1)$を求める場合における、上記アルゴリズムの実行中の途中結果を示す（なお、この場合、ｂ＝１である）。

【００３２】

ここで、法$G=x^4+x+1$であるので、ｍ＝４となる。よって、Ｃ＝１００１１となる。また、除数$a=x+1$であり、ｍ＝４であるので、Ａの初期値は、０００１１とする。被除数ｂ＝１であり、ｍ＝４であるので、Ｂの初期値は、００００１とする。また、Ｄの初期値は００００００、ｎの初期値は０である。

【００３３】

本具体例の場合、Ｄの最終的な値は、０１１１０であるので、求める逆元は、x^3+x^2+1となる。

【００３４】

図７に、上記アルゴリズムをハードウェア化した際の構成を示す。

【００３５】

本アルゴリズムをハードウェア化した場合、この構成は、第１のレジスタＡ（図中、１）、第２のレジスタＣ（図中、２）、第３のレジスタＢ（図中、３）、

第４のレジスタＤ（図中、４）、第５のレジスタｍ（図中、５）、第６のレジスタｎ（図中、６）の６個のレジスタを持つ。また、図中の７～１６の各回路を持つ。また、各レジスタや各回路の制御を行う制御回路（図示せず）を持つ。

【００３６】

レジスタＡは、左シフト回路８と、レジスタＣとの排他的論理和回路７とに接続されており、制御回路（図示せず）に対して最上位ビット（図中、ｍｓｂ）を出力する。

【００３７】

レジスタＣは、レジスタＡを入力として、レジスタＡとの排他的論理和回路７に出力として接続している。

【００３８】

レジスタＢは、標数２の拡大体での２倍演算回路（ｔｗｉｃｅ）１０と、レジスタＤとの排他的論理和回路９とに接続している。

【００３９】

レジスタＤは、レジスタＢと、標数２の拡大体での１／２倍演算回路（ｈａｌｆ）１１と、レジスタＢとの排他的論理和回路９に接続している。

【００４０】

レジスタｍは、デクリメント回路１３と、０か否かを判定する判定回路１２とに接続している。

【００４１】

レジスタｎは、インクリメント回路１６と、デクリメント回路１５と、０か否かを判定する判定回路１４とに接続している。

【００４２】

なお、レジスタＡ～Ｄは、楕円曲線暗号では数百ビット程度を格納でき、レジスタｍ，ｎは、数百程度の値が格納できるビット数を持つ。レジスタＡ～Ｄの長さが２００ビット程度なら、レジスタｍ，ｎは８ビットあれば十分である。

【００４３】

以上の構成でのクリティカルパスは、レジスタｍ，ｎのインクリメント回路とデクリメント回路であり、Ｏ（ｌｏｇ　ｌｏｇ　ｍ）段となる。

【００４４】

このような構成において、前述したアルゴリズム（逆元計算アルゴリズム１）を実行する。すなわち、パラメータの入力、変数の初期化を行った後、第１の状態（ｓｔｅｐ　１）においては、レジスタＡの最上位ビットが１でない限りは、レジスタＡを左シフトし、レジスタＢを標数２の拡大体で２倍し、レジスタｍの内容を１減らし、レジスタｎの内容を１増やすことを繰り返し行うとともに、レジスタＡの最上位ビットが１であるときは、第２の状態（ｓｔｅｐ　２）に状態遷移する。

【００４５】

第２の状態（ｓｔｅｐ　２）においては、レジスタＡに、レジスタＡの内容とレジスタＣの内容の排他的論理和を、レジスタＣに、レジスタＡの内容を、それぞれ格納し、また、レジスタＢに、レジスタＢの内容とレジスタＤの内容の排他的論理和を、レジスタＤに、レジスタＢの内容を、それぞれ格納して、第３の状態（ｓｔｅｐ　３）に状態遷移する。

【００４６】

第３の状態（ｓｔｅｐ　３）においては、レジスタｎの内容が０でない限り、まず、レジスタＡの最上位ビットが１である場合は、レジスタＡに、レジスタＣの内容を排他的論理和で加え、かつ、レジスタＢに、レジスタＤの内容を排他的論理和で加え、他方、レジスタＡの最上位ビットが０である場合は、何もしない。次いで、レジスタｎの内容を１減らし、レジスタＡを左シフトし、レジスタＤを標数２の拡大体で１／２倍することを、繰り返し行うとともに、レジスタｎの内容が０になった場合は、レジスタｍの内容が０でないならば、第１の状態（ｓｔｅｐ　１）に状態遷移し、０であるならば、レジスタＤの内容を結果として出力する。

【００４７】

図８に、上記アルゴリズムをハードウェア化した際の状態遷移図を示す。

【００４８】

初期状態は、ｓｔｅｐ１であり、ｍｓｂ（Ａ）が０の間ｓｔｅｐ１に留まる。

【００４９】

ｍｓｂ（Ａ）が１になると、ｓｔｅｐ２に状態遷移し、ｓｔｅｐ２からは、無条件にｓｔｅｐ３に状態遷移する。

【００５０】

ｎが０でない間、ｓｔｅｐ３に留まり、ｎが０になった際には、ｍの値により、ｍが０でないときはｓｔｅｐ１に戻り、ｍが０であるときは終了する。

【００５１】

以上説明してきたように、本実施形態によれば、標数２のガロア体での逆元計算アルゴリズムをＶＬＳＩ化した際、回路規模や回路遅延を従来よりも小さく抑えることができるようになる。

【００５２】

例えば、法となる多項式の最高次数をｍとしたとき、従来方法のｃｉｒｃｕｉｔ　ｄｅｐｔｈは、ｌｏｇ　ｍであったが、本実施形態によれば、ｌｏｇ　ｌｏｇ　ｍに削減することができる。

【００５３】

また、本実施形態では、全てのシフト操作が、１ビット固定シフトとなる、という利点が得られる。

【００５４】

ここで、図９に、図７の本アルゴリズムをハードウェア化した際の構成と、大部分の部品を共通に利用できる乗算器の構成を示す。この場合、逆元計算装置と、４つのレジスタ、および、１つずつの左シフト回路、排他的論理和回路、２倍演算回路、判定回路、デクリメント回路を共通に利用できる。例えば、図７の逆元計算装置と、レジスタＡ、左シフト回路８、レジスタＢ、レジスタＤ、排他的論理和回路９、２倍演算回路１０、レジスタｍ、判定回路１２、デクリメント回路１３の各部品を共通に利用できる。新たに必要となる部品は、論理積回路２０の一つだけである。

【００５５】

以下に、Ｂ←Ａ×Ｄを計算する乗算アルゴリズムを示す。

【００５６】

入力は、Ａ，Ｄ，Ｇ，ｍ（Ｇはｍ次多項式、ＡとＤは次数がｍより小さい多項

式）である。

【００５７】

＜乗算アルゴリズム＞

パラメータの値の入力

B ＝ 0

while m ≠ 0

m ← m-1

B ← twice(B)

A ← left_shift(A)

if msb(A) ＝ 1 then B ← B xor D

wend

Bを出力する

＜乗算アルゴリズム＞

ところで、本実施形態のレジスタｍとレジスタｎをワンホットカウンタで実現することにより、入力が何ビットであっても全体として回路遅延が定数段となる逆元計算回路とすることができる。

【００５８】

図１０に、ワンホットカウンタの例を示す。

【００５９】

ワンホットカウンタでは、ｍ＋１個のレジスタのうち１つだけある１が格納されたレジスタの番号で数を表現する。図１０では、番号２のレジスタに１が格納されているので数２を表現している。

【００６０】

ワンホットカウンタでは、

１）表現している数を１増やす操作は左シフトである、

２）表現している数を１減らす操作は右シフトである、

３）表現している数がある特定の数であるかどうかを判定するのは特定のビットが１であるかどうかを判定するだけでよい、

という３つの特徴があり、これらのいずれの操作も回路遅延は定数段である。

【００６１】

さて、先に示した逆元計算アルゴリズム１やこれをフローチャートで表した図１は、種々変形して実施することが可能である。

【００６２】

以下では、先に示した逆元計算アルゴリズム１のループを一重にすることでハードウェア化しやすくした実施形態を示す。

【００６３】

この場合の逆元計算アルゴリズムを以下に示す。

【００６４】

＜逆元計算アルゴリズム２＞

入力　A,B,G,m（Gはm次多項式、AとBは次数がmより小さい多項式）

```
C ← G
D ← 0
n ← 0
state ← 1
while m≠0 and n≠0
  f ← msb(A)
  if f = 1 then
      if state = 1 then
          (A, C) ← (A xor C, A)
          (B, D) ← (B xor D, B)
      else
          A ← A xor C
          B ← B xor D
      endif
  endif

  A ← left_shift(A)
```

```
    if  state  =  1  and  (f = 0 or n = 0)  then
        m  ←  m-1
        n  ←  n+1
        B  ←  twice(B)
    else
        n  ←  n-1
        D  ←  half(D)
        if  n  =  0  then  state ← 1  else  state ← 0
    endif
  wend
  Dを出力する
```

＜逆元計算アルゴリズム２＞

以上のアルゴリズムの記述をフローチャートの形で表したのが図１１である。

【００６５】

このアルゴリズム（逆元計算アルゴリズム２）は、先に説明したアルゴリズム（逆元計算アルゴリズム１）に比較して、ｓｔａｔｅおよびｆという１ビットの変数が増えている。途中でＡが書き換わっているので、ｆはｍｓｂ（Ａ）を保持しておくものである（ただし、ハードウェア化した際には必要なくなる）。ｓｔａｔｅは、逆元計算アルゴリズム１の内側にある二つのループのいずれを回っているかを表している（状態を記憶しているので、ハードウェア化した際には記憶装置が必要になる）。ｆ＝１のときが最初のループ（ｓｔｅｐ　１）とｓｔｅｐ２の状態にいて、ｆ＝０のときが後の方のループ（ｓｔｅｐ　３）にいることを示している。

【００６６】

この逆元計算アルゴリズム２についても、これをハードウェア化した際の構成は、図７と同じである。

【００６７】

また、この場合も、図７の部品を利用し、これに論理和回路２０を追加して、図９及び前述の乗算アルゴリズムで示した乗算器が構成可能である。

【００６８】

なお、この逆元計算アルゴリズムの実行中の各レジスタの途中結果は、基本的には、図６と同様である。

【００６９】

また、逆元計算アルゴリズム１，２以外にも、それらと等価なアルゴリズムになるように、種々変形して実施することが可能である。この場合にも、これまで説明してきたと同様の作用効果を得ることができる。

【００７０】

なお、以上の各機能は、ソフトウェアとして実現可能である。

また、本実施形態は、コンピュータに所定の手段を実行させるための（あるいはコンピュータを所定の手段として機能させるための、あるいはコンピュータに所定の機能を実現させるための）プログラムとして実施することもでき、該プログラムを記録したコンピュータ読取り可能な記録媒体として実施することもできる。

【００７１】

なお、この発明の実施の形態で例示した構成は一例であって、それ以外の構成を排除する趣旨のものではなく、例示した構成の一部を他のもので置き換えたり、例示した構成の一部を省いたり、例示した構成に別の機能あるいは要素を付加したり、それらを組み合わせたりすることなどによって得られる別の構成も可能である。また、例示した構成と論理的に等価な別の構成、例示した構成と論理的に等価な部分を含む別の構成、例示した構成の要部と論理的に等価な別の構成なども可能である。また、例示した構成と同一もしくは類似の目的を達成する別の構成、例示した構成と同一もしくは類似の効果を奏する別の構成なども可能である。

また、この発明の実施の形態で例示した各種構成部分についての各種バリエーションは、適宜組み合わせて実施することが可能である。

また、この発明の実施の形態は、個別装置としての発明、関連を持つ２以上の装置についての発明、システム全体としての発明、個別装置内部の構成部分についての発明、またはそれらに対応する方法の発明等、種々の観点、段階、概念ま

たはカテゴリに係る発明を包含・内在するものである。

従って、この発明の実施の形態に開示した内容からは、例示した構成に限定されることなく発明を抽出することができるものである。

【００７２】

本発明は、上述した実施の形態に限定されるものではなく、その技術的範囲において種々変形して実施することができる。

【００７３】

【発明の効果】

本発明によれば、標数２のガロア体での逆元計算アルゴリズムをＶＬＳＩ化した際、回路規模や回路遅延を従来よりも小さく抑えることができるようになる。

【図面の簡単な説明】

【図１】

本発明の一実施形態に係る標数２の拡大体での逆元計算アルゴリズムの一例を示すフローチャート

【図２】

同実施形態に係る多項式の表現について説明するための図

【図３】

同実施形態に係るｌｅｆｔ＿ｓｈｉｆｔについて説明するための図

【図４】

同実施形態に係るｔｗｉｃｅについて説明するための図

【図５】

同実施形態に係るｈａｌｆについて説明するための図

【図６】

同実施形態に係る逆元計算アルゴリズムについて説明するための図

【図７】

同実施形態に係る逆元計算アルゴリズムをハードウェア化した際の構成例を示す図

【図８】

同実施形態に係る逆元計算アルゴリズムをハードウェア化した際の状態遷移の

一例を示す図

【図９】

同実施形態に係る逆元計算アルゴリズムをハードウェア化した際の構成と大部分の部品を共通に利用できる乗算器の構成例を示す図

【図１０】

同実施形態に係るワンホットカウンタの例を示す図

【図１１】

同実施形態に係る標数２の拡大体での逆元計算アルゴリズムの他の例を示すフローチャート

【符号の説明】

１～６…レジスタ

７，９…排他的論理和回路

８…左シフト回路

１０…２倍演算回路

１１…１／２倍演算回路

１２，１４…判定回路

１３…デクリメント回路

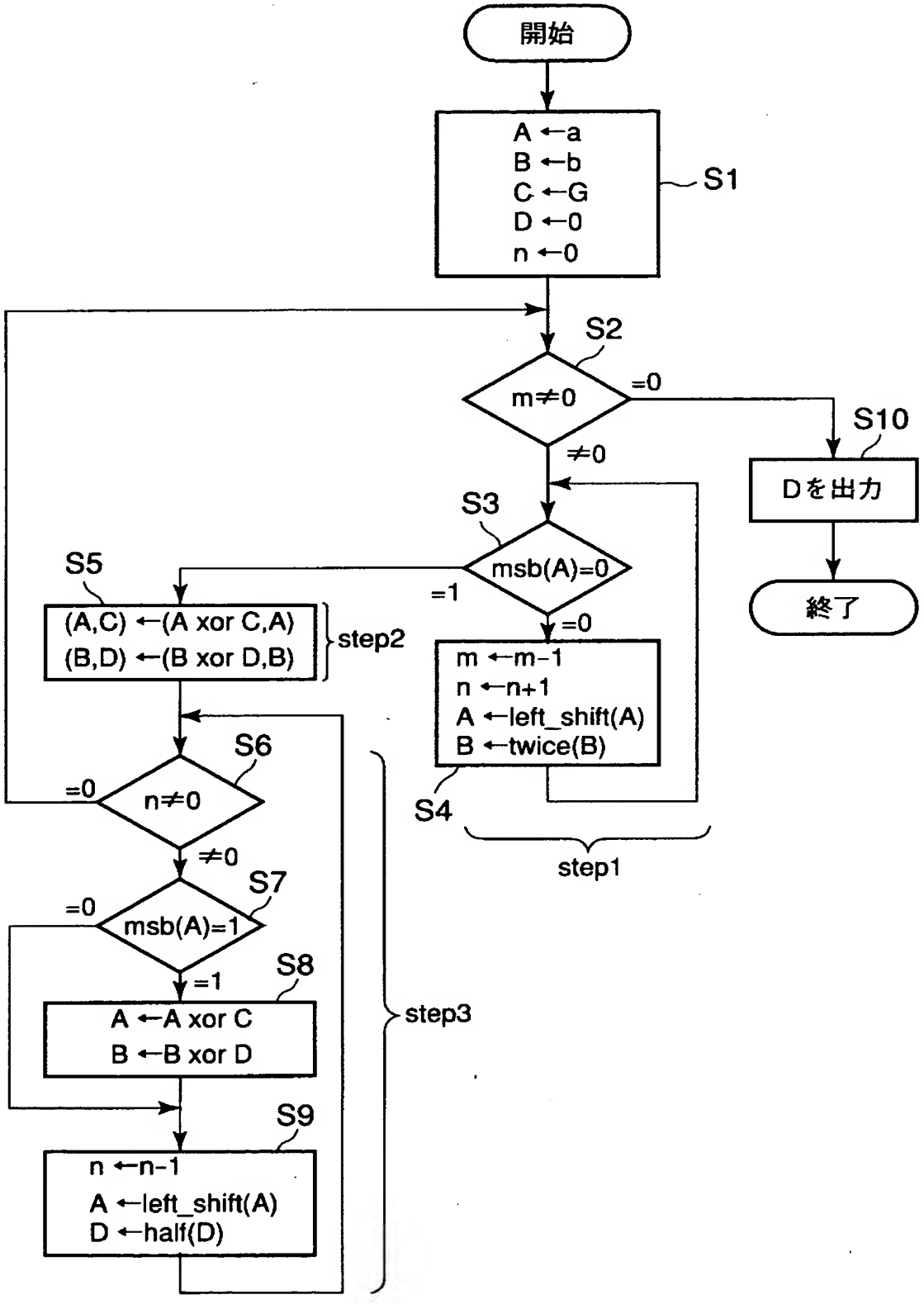
１５…デクリメント回路

１６…インクリメント回路

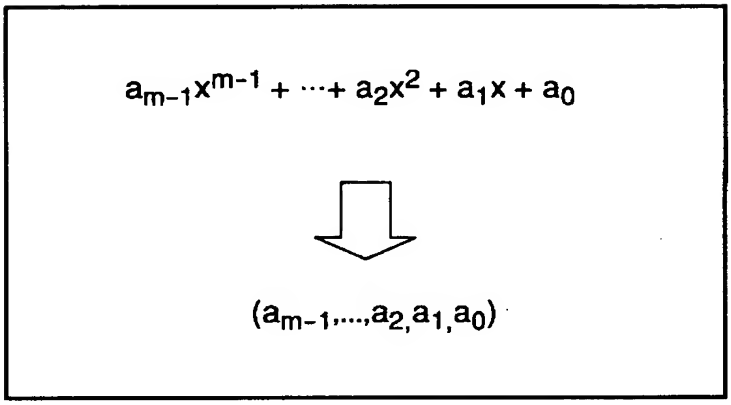
２０…論理積回路

【書類名】　　図面

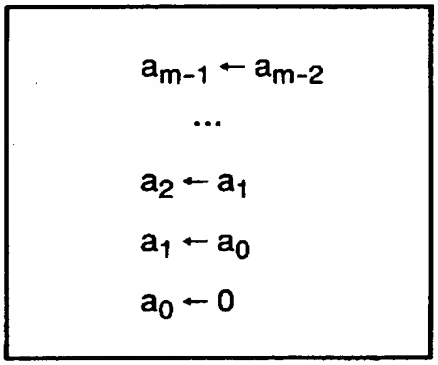
【図１】


開始
A ←a
B ←b
C ←G
D ←0
n ←0
S1
S2
m≠0
=0
≠0
S10
Dを出力
終了
S3
msb(A)=0
=1
=0
S5
(A,C) ←(A xor C,A)
(B,D) ←(B xor D,B)
step2
m ←m−1
n ←n+1
A ←left_shift(A)
B ←twice(B)
S4
step1
S6
n≠0
=0
≠0
S7
msb(A)=1
=0
=1
S8
A ←A xor C
B ←B xor D
step3
S9
n ←n−1
A ←left_shift(A)
D ←half(D)

【図２】

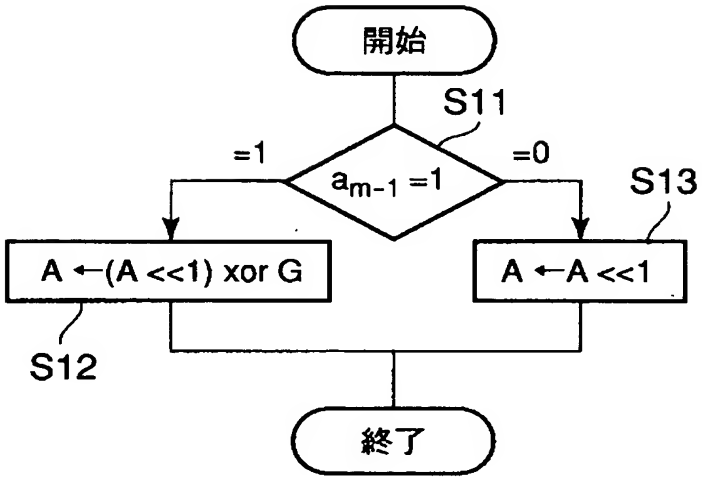


【図３】

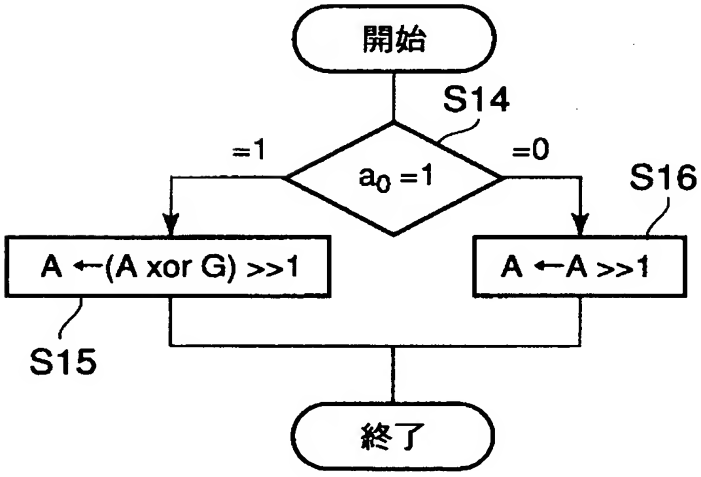


出証特２００３－３００９７０７

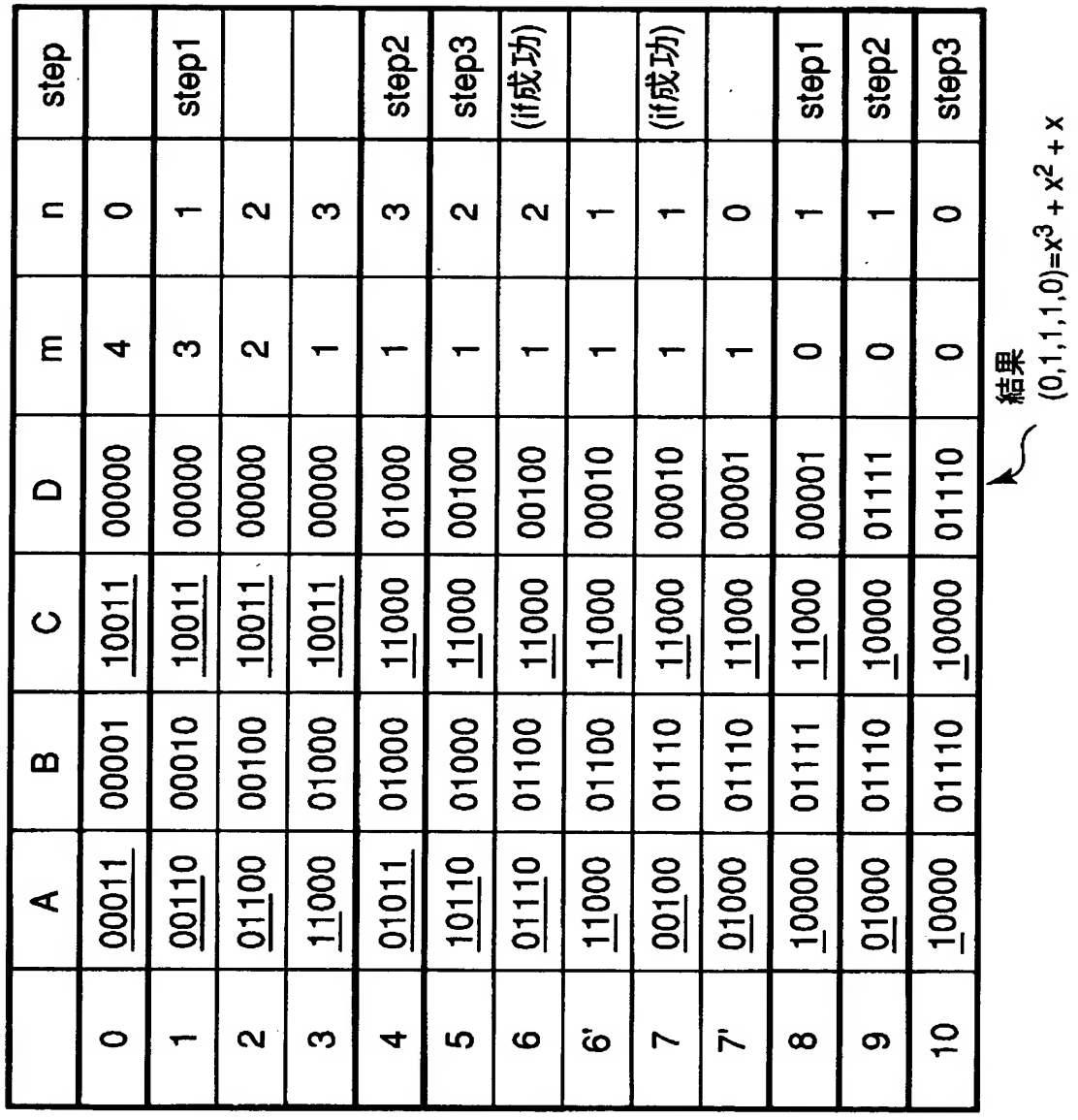
【図４】


開始
S11
=1
a_{m-1} =1
=0
S13
A ←(A <<1) xor G
A ←A <<1
S12
終了

【図５】


開始
S14
=1
a_0 =1
=0
S16
A ←(A xor G) >>1
A ←A >>1
S15
終了

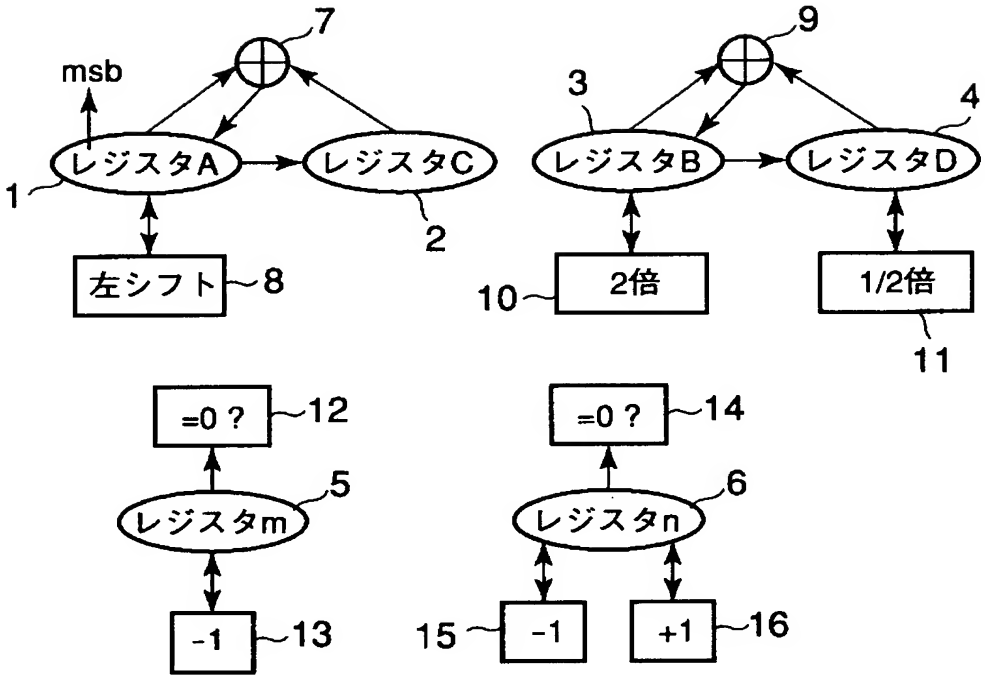
【図６】



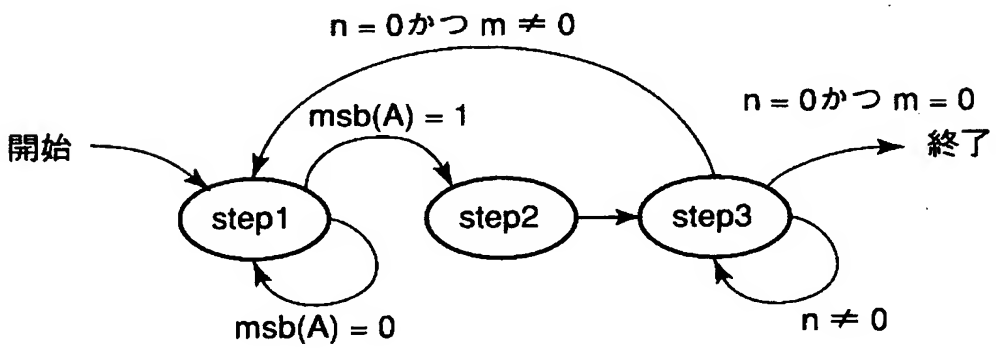
	A	B	C	D	m	n	step
0	00011	00001	10011	00000	4	0	
1	00110	00010	10011	00000	3	1	step1
2	01100	00100	10011	00000	2	2	
3	11000	01000	10011	00000	1	3	
4	01011	01000	11000	01000	1	3	step2
5	10110	01000	11000	00100	1	2	step3
6	01110	01100	11000	00100	1	2	(if成功)
6'	11000	01100	11000	00010	1	1	
7	00100	01110	11000	00010	1	1	(if成功)
7'	01000	01110	11000	00001	1	0	
8	10000	01111	11000	00001	0	1	step1
9	01000	01110	10000	01111	0	1	step2
10	10000	01110	10000	01110	0	0	step3

結果
$(0,1,1,1,0)=x^3+x^2+x$

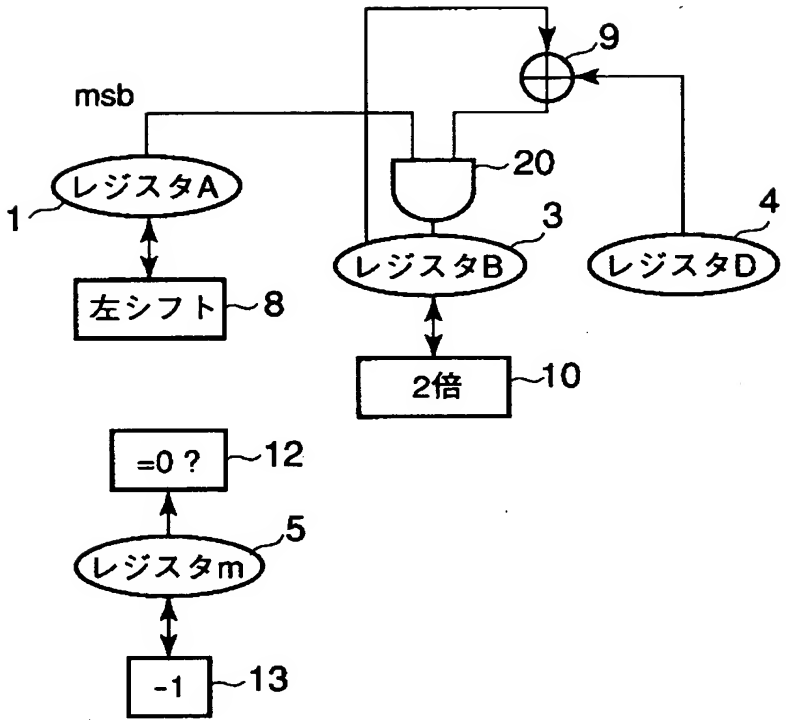
【図７】


7
msb
レジスタA
1
レジスタC
2
左シフト
8
9
3
4
レジスタB
レジスタD
10
2倍
1/2倍
11
=0？
12
5
レジスタm
-1
13
=0？
14
6
レジスタn
15
-1
+1
16

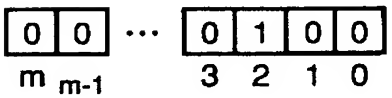
【図８】


n = 0かつ m ≠ 0
msb(A) = 1
n = 0かつ m = 0
開始
終了
step1
step2
step3
msb(A) = 0
n ≠ 0

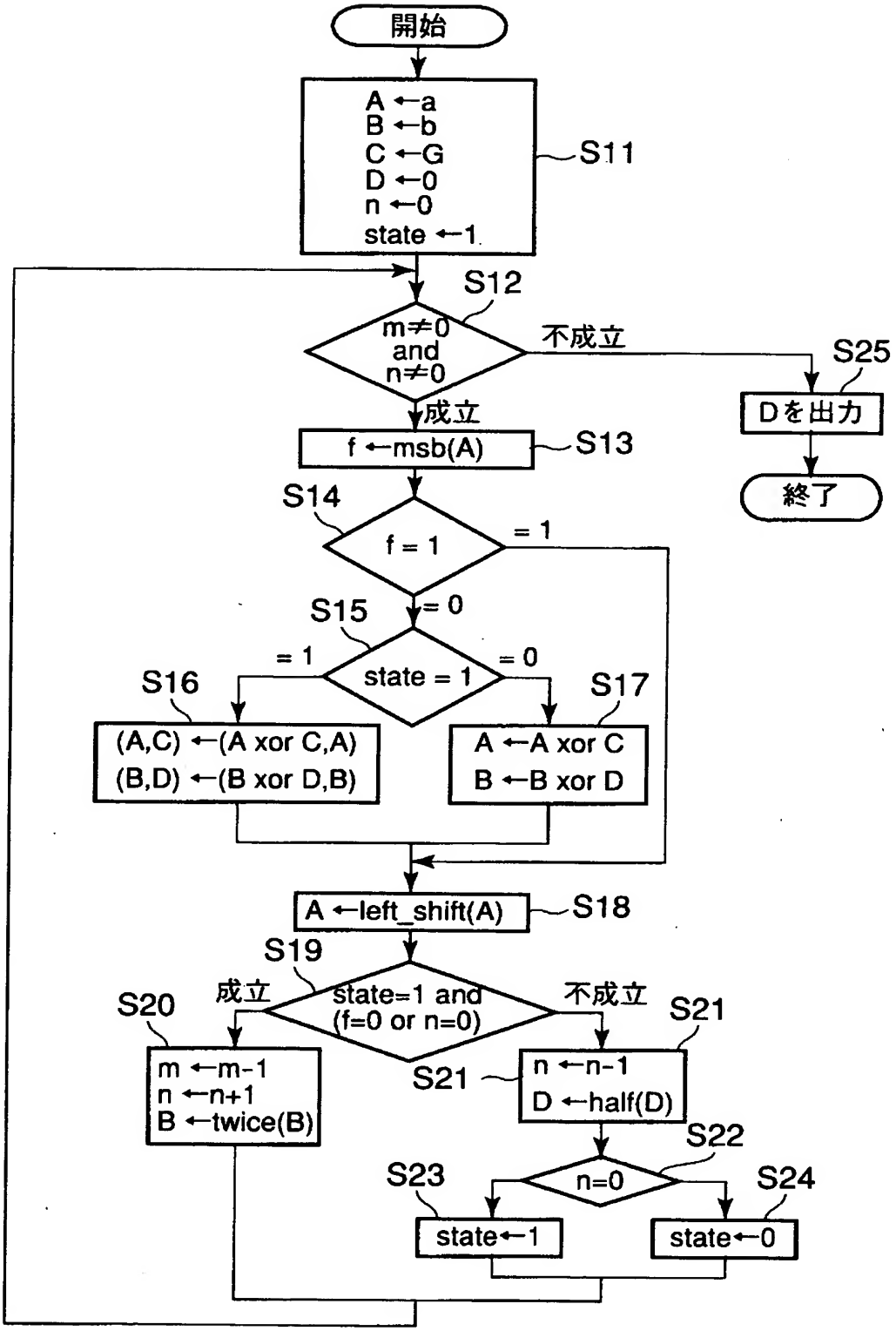
【図９】


9
msb
20
レジスタA
1
3
4
レジスタB
レジスタD
左シフト
8
2倍
10
=0？
12
5
レジスタm
-1
13

【図１０】


0 0 … 0 1 0 0
m m-1 3 2 1 0

【図１１】


開始
A ←a
B ←b
C ←G
D ←0
n ←0
state ←1
S11
S12
m≠0 and n≠0
不成立
成立
S25
Dを出力
終了
f ←msb(A)
S13
S14
f = 1
= 1
= 0
S15
= 1
state = 1
= 0
S16
S17
(A,C) ←(A xor C,A)
(B,D) ←(B xor D,B)
A ←A xor C
B ←B xor D
A ←left_shift(A)
S18
S19
成立
state=1 and (f=0 or n=0)
不成立
S20
S21
m ←m-1
n ←n+1
B ←twice(B)
S21
n ←n-1
D ←half(D)
S22
n=0
S23
S24
state←1
state←0

【書類名】　　要約書

【要約】

【課題】　標数２のガロア体での逆元計算アルゴリズムをＶＬＳＩ化した際、回路規模や回路遅延をより小さく抑えられる逆元計算装置を提供すること。

【解決手段】　第１乃至第６のレジスタ（１～６）と、左シフト回路（８）と、排他的論理和回路（７，９）と、標数２の拡大体での２倍演算を施す２倍演算回路（１０）と、標数２の拡大体での１／２倍演算を施す１／２倍演算回路（１１）と、レジスタの内容が０か否か判定する判定回路（１２，１４）と、レジスタの内容をデクリメントするデクリメント回路（１３，１５）と、レジスタの内容をインクリメントするインクリメント回路（１６）と、それらを制御する制御回路とを用いて構成する。

【選択図】　　図１

出　願　人　履　歴　情　報

識別番号　　〔０００００３０７８〕

１．変更年月日　　２００１年　７月　２日
［変更理由］　住所変更
住　所　　東京都港区芝浦一丁目１番１号
氏　名　　株式会社東芝